Claims:

Claim 1

A user authentication method, whereby a one-way function F, which should satisfy $v = F(g, -s)$, is determined by employing an integer g that is defined in advance for a relation between a public key v and a secret key s of a prover computer, and whereby a relation is verified between said prover computer and each of multiple verifier computers, comprising the steps of:

said prover computer generating a random number a, obtaining a cryptogram A = the function $F(g, a)$, and transmitting said cryptogram A to said verifier computers;

said verifier computers generating a random number b, obtaining a cryptogram B = the function $F(g, b)$ and a cryptogram X = the function $F(A, b)$, and transmitting said cryptograms B and X to said prover computer;

said prover computer determining whether a relation of said cryptogram X = the function $F(B, a)$ has been established and generating a random number c when said relation has been established, obtaining a cryptogram C = the function $F(g, c)$ and a cryptogram Y = the function $F(B, c)$, or a cryptogram C = the function $F(A, c)$, a cryptogram Y = the function $F(X, c)$ and a cryptogram Z = a function $H(a, Y, s)$, and transmitting said cryptograms C and Y or said cryptograms C, Y and Z to said verifier computers; and

said verifier computers, when said cryptogram Y = the function $F(C, b)$ and said cryptogram A = a function

$J(v, Y, g, Z)$ are established, determining that said relation between said prover computer and said verifier computer is correct.

Claim 2

The user authentication method according to claim 1, wherein said public key v is obtained by employing prime numbers p and q that satisfy $(q|p - 1)$, and by defining an element of the order q as said integer g.

Claim 3

The user authentication method according to claim 1, wherein, by using said public key v and said secret key s, said function F acquires a relation $v = F(g, -s) = g^{-s} \bmod p$.

Claim 4

The user authentication method according to claim 1, wherein, when a relation $X = B^{a} \bmod p$ is established, said prover computer generates said random number c.

Claim 5

The user authentication method according to claim 1, wherein said function H has a relation $H(a, Y, s) = a + Ys \bmod q$.

Claim 6

The user authentication method according to claim 1, wherein said function J has a relation $J(v, Y, g, Z) = v^{Y}g^{Z} \bmod p$.

Claim 7

A storage medium on which a user authentication program, which is to be read by a prover computer, is stored whereby a one-way function F, which should satisfy v = F(g, -s), is determined by employing an integer g, which is defined in advance for the relation between a public key v and a secret key s of said prover computer, and whereby a relation is verified between said prover computer and each of multiple verifier computers, said user authentication program permitting said prover computer to perform:

a process for generating a random number a and for obtaining a cryptogram A = the function F(g, a), and for transmitting said cryptogram A to said verifier computers;

a process for receiving cryptograms B and X from said verifier computer, and for employing said cryptograms to determine whether a relation a cryptogram X = the function F (B, a) has been established;

a process for generating a random number c when said relation has been established; and

a process for obtaining a cryptogram C = the function F(g, c) and a cryptogram Y = the function F(B, c), or a cryptogram C = the function F(A, c), a cryptogram Y = the function F(X, c) and a cryptogram Z = the function H(a, Y, s); and

a process for transmitting said cryptograms C and Y, or C, Y and Z, to said verifier computers.

Claim 8

A storage medium on which a user authentication program, which is to be read by a prover computer, is stored whereby a one-way function F, which should satisfy v = F(g, -s), is determined by employing an integer g, which is defined in advance for the relation between a public key v and a secret key s of said prover computer, and whereby a relation is verified between said prover computer and each of multiple verifier computers, said user authentication program permitting said verifier computers to perform:

a process for receiving a cryptogram A from said prover computer and for generating a random number b;

a process for obtaining a cryptogram B = the function F(g, b) and a cryptogram X = the function F(A, b), using said random number b and said cryptogram that is received, and for transmitting said cryptograms B and X to said prover computer;

a process for receiving, from said prover computer, a cryptogram C = the function F(g, c) and a cryptogram Y = the function F(B, c), or a cryptogram C = the function F(A, c), a cryptogram Y = the function F(X, c) and a cryptogram Z = the function H(a, Y, s); and

a process, based on said cryptograms C and Y or C, Y and Z that are received, for verifying a relation between said verifier computer and said prover computer when two relations of said cryptogram Y = the function F(C, b) and said cryptogram A = the function J(v, Y, g, Z) are established at the same time.

Claim 9

A user authentication apparatus for a prover computer, wherein a one-way function F, which should satisfy v = F(g, -s), is determined by employing an integer g, which is defined in advance, for a relation between a public key v and a secret key s of said prover computer, and wherein a relation is verified between said prover computer and each of multiple verifier computers, said user authentication apparatus comprising:

transmission means, for generating a random number a and obtaining a cryptogram A = the function F(g, a), and for transmitting said obtained cryptogram A to said verifier computers;

reception means, for receiving cryptograms B and X from said verifier computers;

verification means, for employing said cryptograms B and X to determine whether a relation of said cryptogram X = the function F(B, a) has been established;

cryptogram computation means, for generating a random number c when it has been ascertained that said relation has been established, and for obtaining a cryptogram C = the function F(g, c) and a cryptogram Y = the function F(B, c), or a cryptogram C = the function F(A, c), a cryptogram Y = the function F(X, c) and a cryptogram Z = the function H(a, Y, s); and

cryptogram transmission means, for transmitting said cryptograms C and Y or C, Y and Z to said verifier computers.

Claim 10

A user authentication apparatus for a prover computer wherein a one-way function F, which should satisfy v = F(g, -s), is determined by employing an integer g, which is defined in advance, for the relation between a public key v and a secret key s of a prover computer, and wherein a relation is verified between said prover computer and each of multiple verifier computers, said user authentication apparatus comprising:

reception means, for receiving a cryptogram A from said prover computer;

transmission means, for generating a random number b, and for employing said random number b and said cryptogram A that is received to obtain a cryptogram B = the function F(g, b) and a cryptogram X = the function F(A, b), and for transmitting said cryptograms B and X to said prover computer;

cryptogram reception means, for receiving from said prover computer a cryptogram C = the function F(g, c) and a cryptogram Y = the function F(B, c) or a cryptogram C = the function F(A, c), a cryptogram Y = the function F(X, c), and a cryptogram Z = the function H(a, Y, s); and

verification means, for performing a procedure, based on said cryptograms C, Y and Z that are received, for verifying a relation between said verifier computers and said prover computer when two relations of said cryptogram Y = the function F(C, b) and said cryptogram A = the function J(v, Y, g, Z) are established at the same time.

Claim 11

A user authentication system comprising:

the user authentication apparatus for said prover computer according to claim 9; and

a plurality of user authentication apparatuses for said verifier computers according to claim 10.

Claim 12

A user authentication system, wherein a one-way function F, which should satisfy v = F(g, -s), is determined by employing an integer g, which is defined in advance, for the relation between a public key v and a secret key s of a prover computer, and wherein a relation is verified between said prover computer and each of multiple verifier computers, comprising:

transmission means, for said prover computer, for generating a random number a and obtaining a cryptogram A = the function F(g, a), and for transmitting said obtained cryptogram A to said verifier computers;

reception means for said verifier computers, for receiving said cryptogram A from said prover computer;

transmission means for said verifier computers, for generating a random number b with which said cryptogram A is employed to obtain a cryptogram B = the function F(g, b) and a cryptogram X = the function F(A, b), and for transmitting said cryptograms B and X to said prover computer;

reception means for said prover computer, for receiving said cryptograms B and X from said verifier computers;

verification means for said prover computer, for employing said cryptograms B and X to determine whether a relation of said cryptogram X = the function F(B, a) has been established;

cryptogram computation means for said prover computer, for generating a random number c when it is ascertained that said relation has been established, and for obtaining said cryptogram C = the function F(g, c) and said cryptogram Y = the function F(B, c), or said cryptogram C = the function F(A, c) and said cryptogram Y = the function F(X, c), and a cryptogram Z = the function H(a, Y, s); and

cryptogram transmission means for said prover computer, for transmitting said cryptograms C, Y and Z to said verifier computers;

cryptogram reception means, for said verifier computers, for receiving said cryptograms C, Y and Z from said prover computer; and

verification means for said verifier computers, for employing said cryptograms C, Y and Z that are received to verify a relation between said verifier computers and said prover computer when two relations of said cryptogram Y = the function F(C, b) and said cryptogram A = the function J(v, Y, g, Z) are established at the same time.

13. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing user authentication, the

computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the apparatus of claim 9.

14. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing user authentication, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the apparatus of claim 10.

15. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing user authentication, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the system of claim 11.

16. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing user authentication, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the system of claim 12.

17. An article of manufacture comprising a computer

usable medium having computer readable program code means embodied therein for implementing a user authentication method, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 1.